RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: IDY-M02

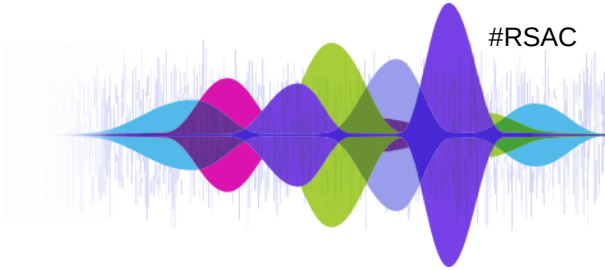
Time’s up on Standing Access: Making JIT Happen with Identity Data & GenAI

Matthew Sullivan

Infrastructure Security and Identity Team Lead
Instacart

Dominic Zanardi

Sr. Security Engineer II
Instacart



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

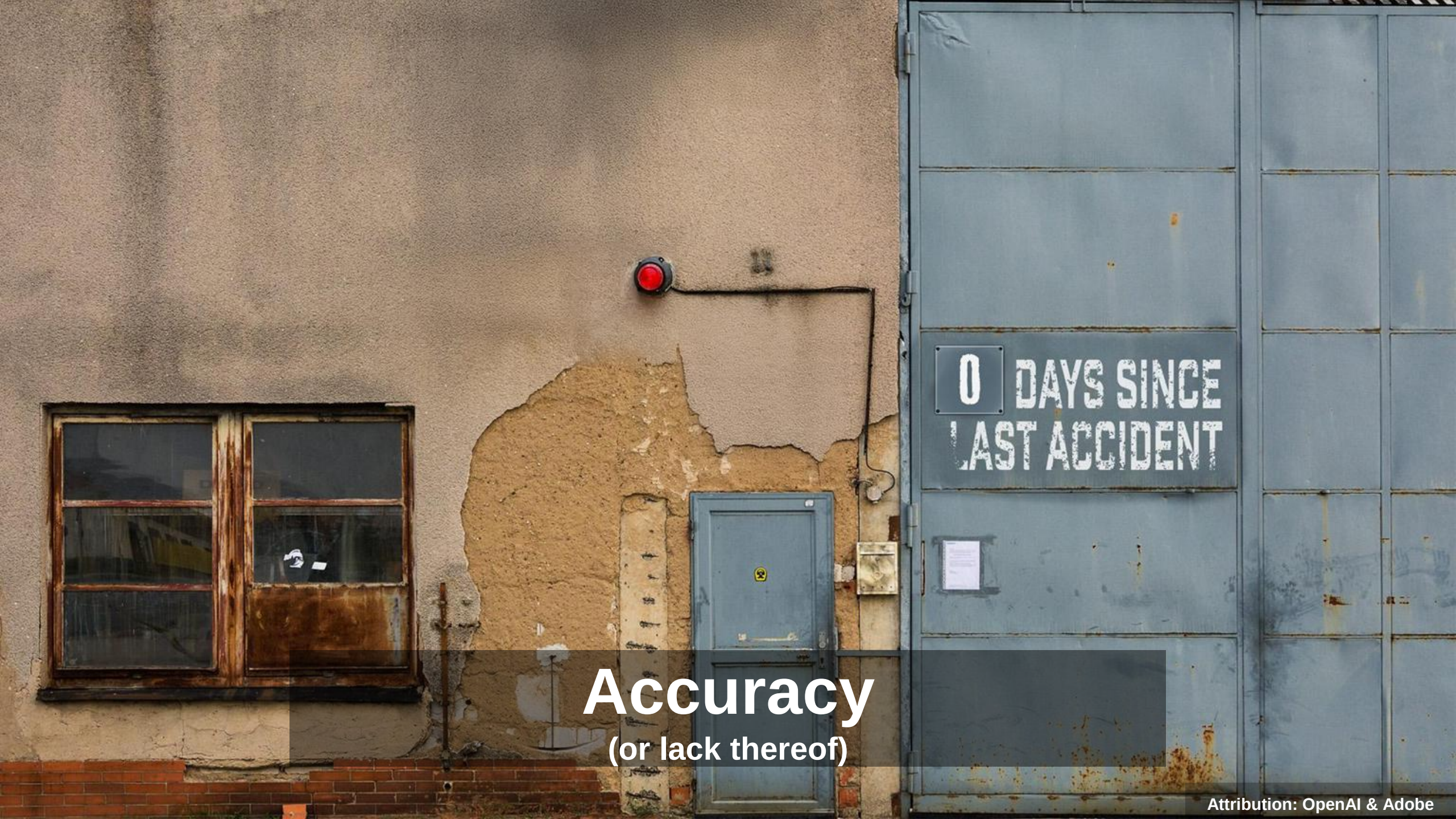
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Attribution: OpenAI & Adobe

Attribution: OpenAI & Adobe

Tolerance for Risk

Attribution: OpenAI & Adobe

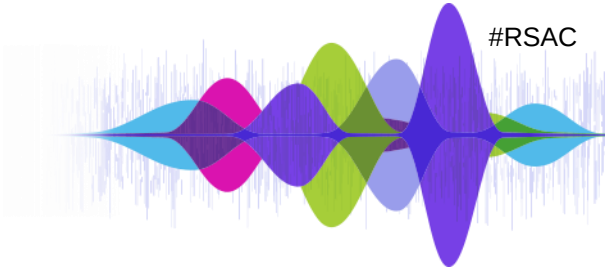


Accuracy

(or lack thereof)

Attribution: OpenAI & Adobe

Evolving Risk Landscape

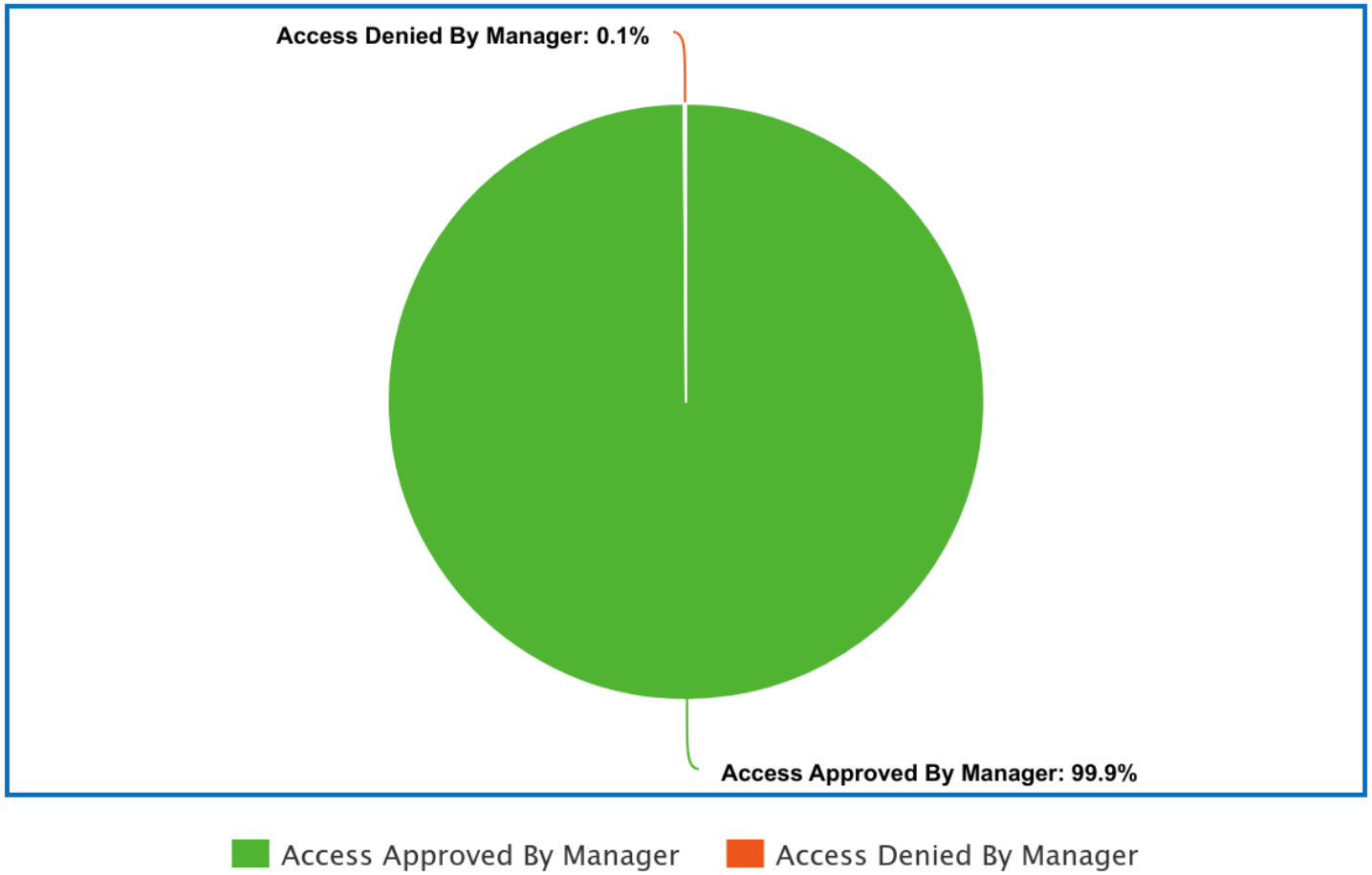


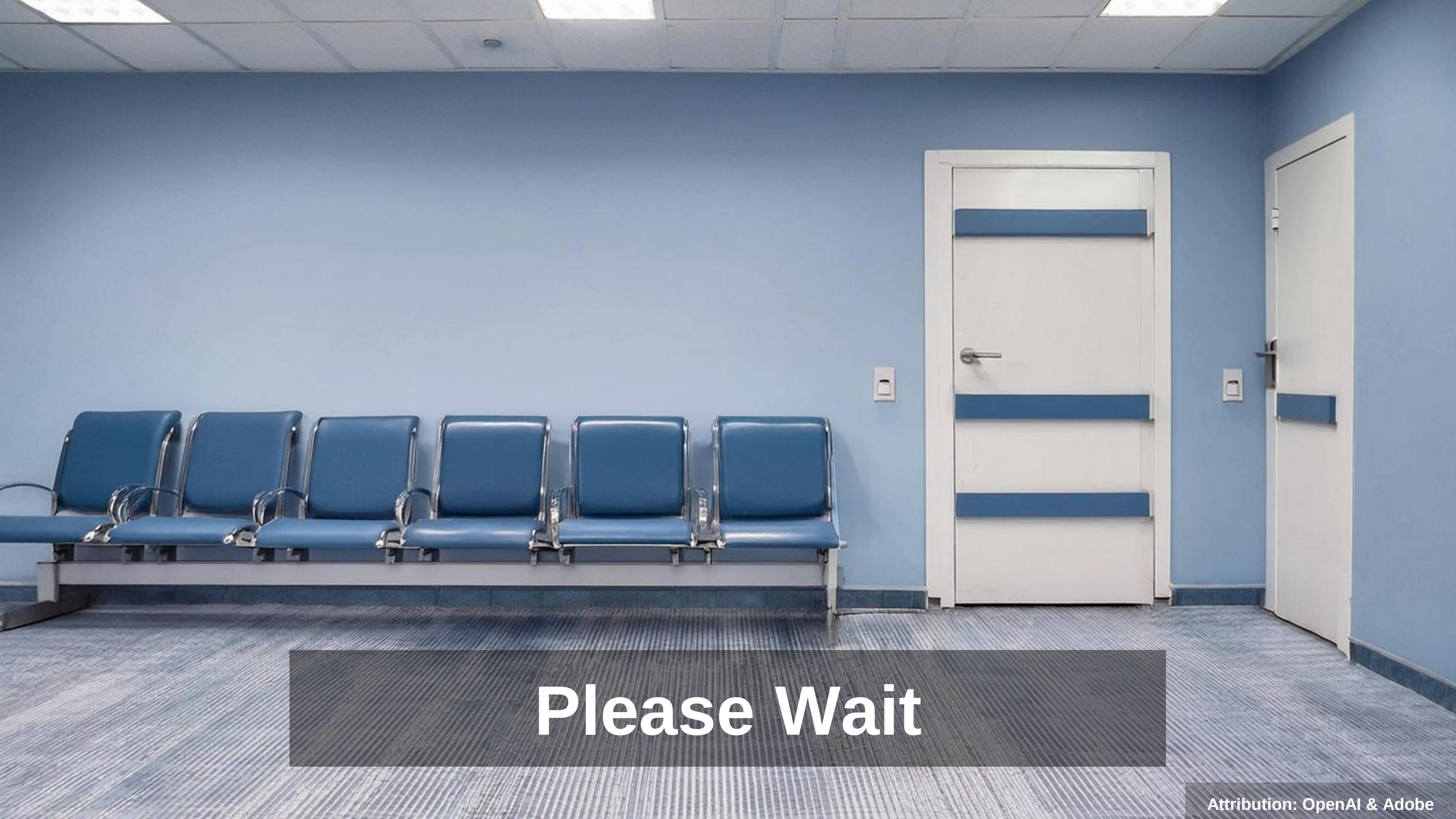
- IDC Research claims **79%** of organizations face operational inefficiencies and elevated risk due to excessive always-on access.
- Microsoft Security Research published that identity-based attacks involving excessive privilege accounted for **61%** of total breaches.
- Recent SANS Institute study claims that implementing JIT as part of a Zero-Trust framework drops threat exposure by **40%**.

High Quality
=
Hard Work

Attribution: OpenAI & Adobe

Status Quo of Manager Approvals





Attribution: OpenAI & Adobe

User Experience Challenges

Comment	I may have selected the wrong access level and require only read only access for my job - can this be switched in my request to move along my access approval?

Attribution: OpenAI & Adobe

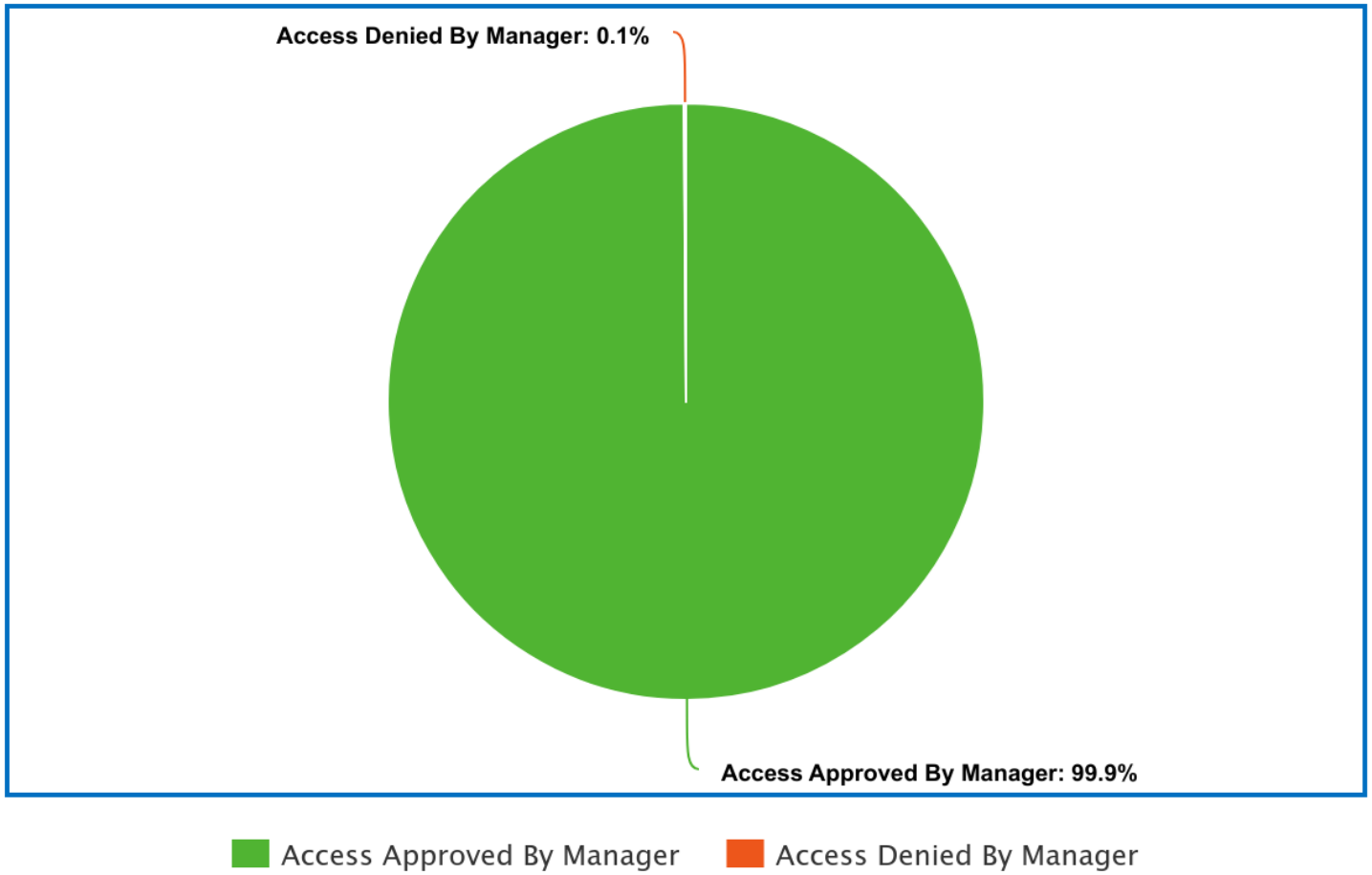
Modern Identity Program: Table Stakes

- Relationships
- Business processes
- Infrastructure as Code

Modern Identity Program: No Access Reviews

- Access reviews look *back*.
- Protect forward.
- Yes, you can pass your audit.

Status Quo of Manager Approvals



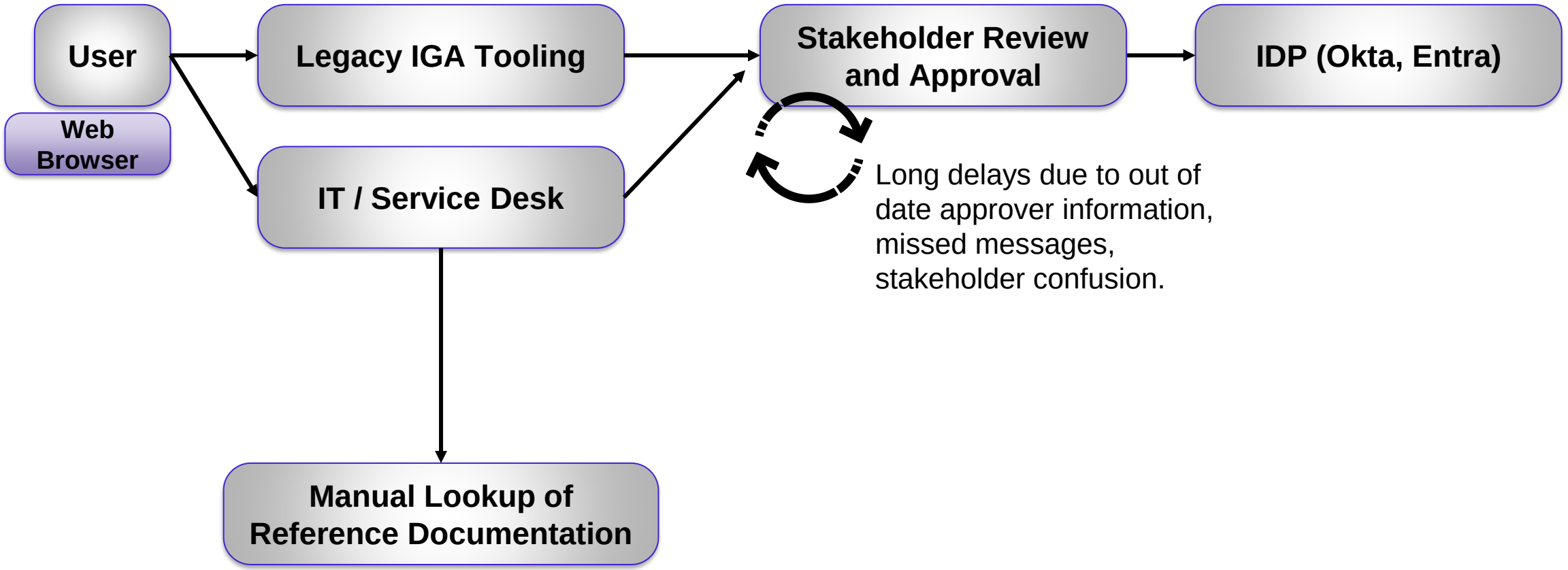
Instacart's Implementation

- Needed new technology
  - ConductorOne, Opal, StrongDM, Okta IGA
- New ways of working
- Datamining to success

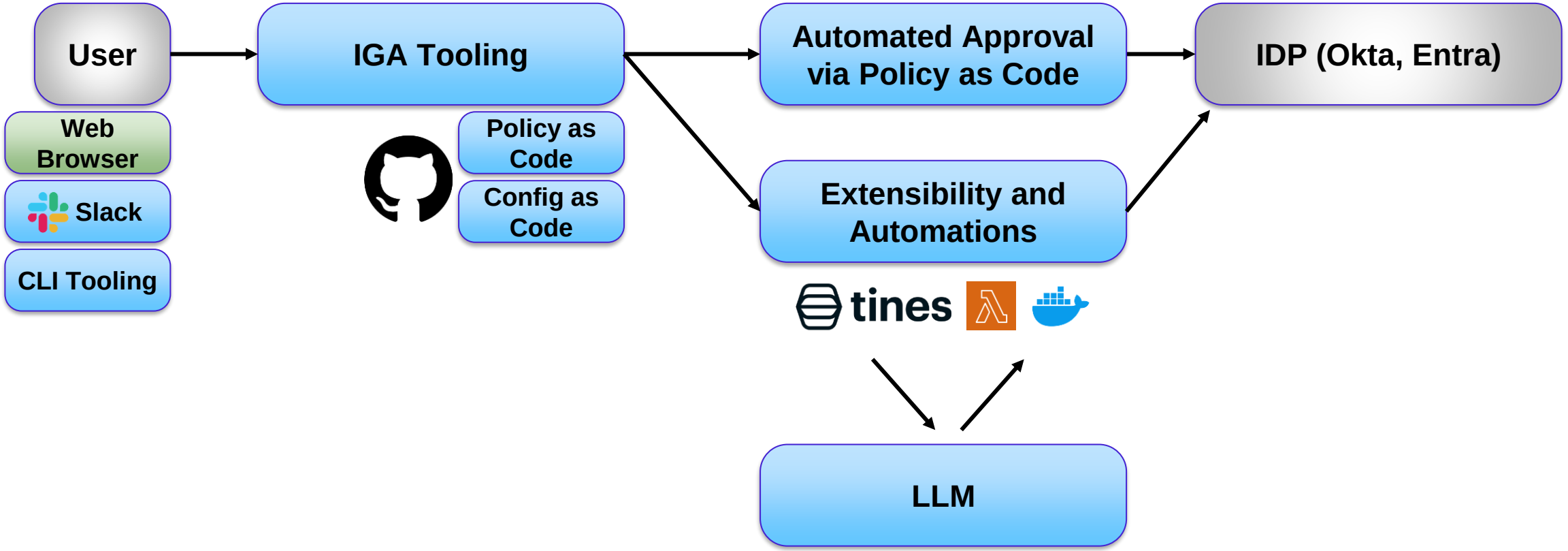
Our AI Identity Tooling Stack

- User experience assistance
  - Request accuracy
  - Out of office
- Role engineering
- AI *assisted* “gray area” automated access approvals
  - “Gadjit”, the open-source access review bot

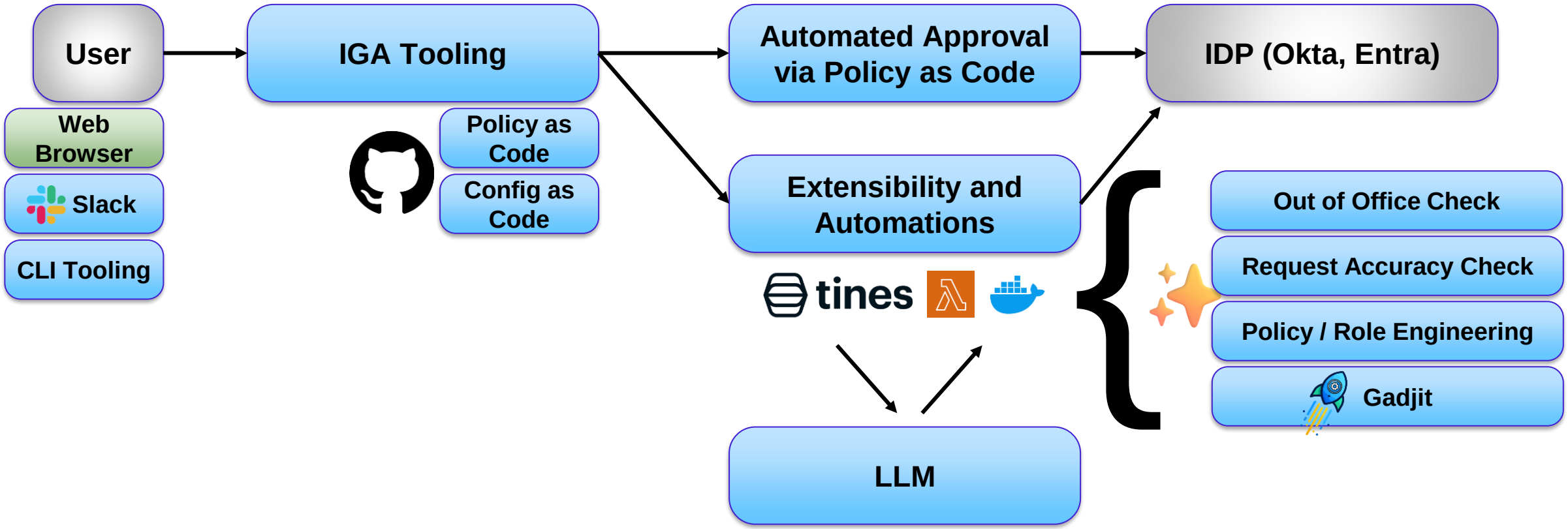
Traditional Identity Architecture


User
Web Browser
Legacy IGA Tooling
IT / Service Desk
Manual Lookup of Reference Documentation
Stakeholder Review and Approval
IDP (Okta, Entra)
Long delays due to out of date approver information, missed messages, stakeholder confusion.

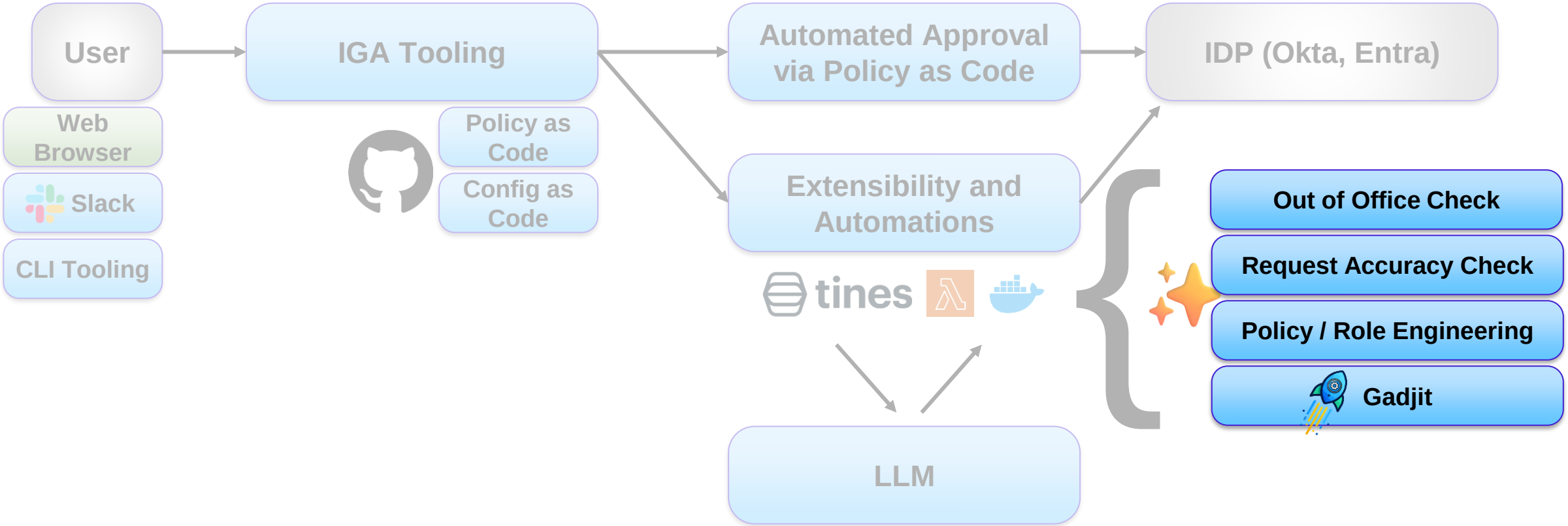
Instacart's Modern Identity Architecture



Instacart's Modern Identity Architecture

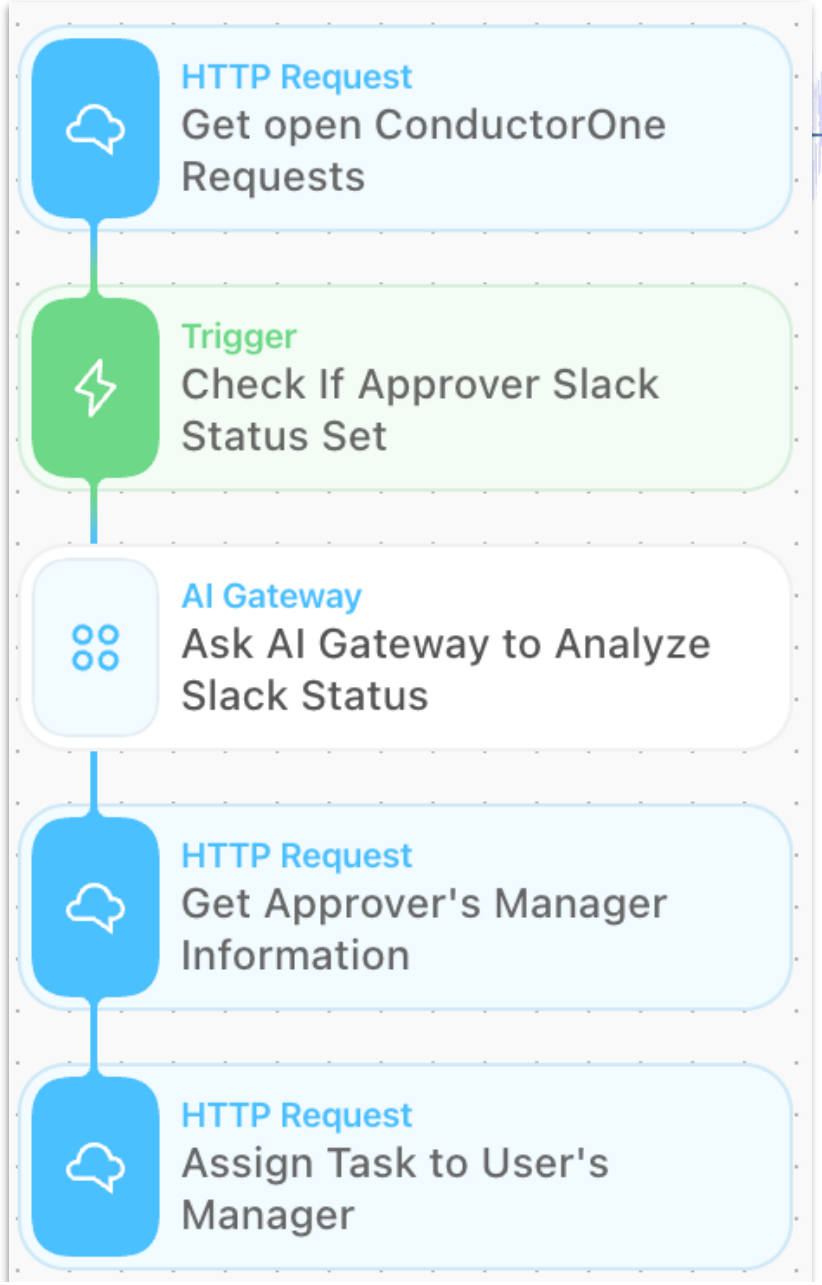


Instacart's Modern Identity Architecture



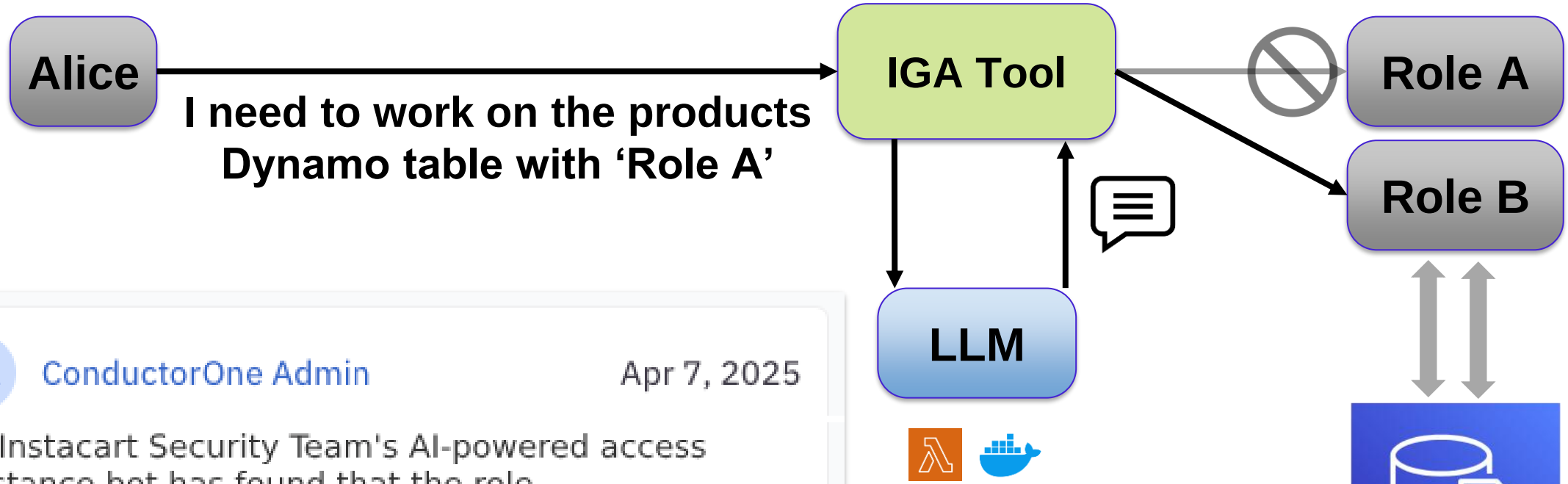
Out of Office

- End-user experience is *crucial*
- Use an LLM to determine how long user may be out
- Redirect to skip-level manager



** simplified for demo purposes; there are other checks, such as avoiding re-assigning approvals to executives*

Request Accuracy & Redirection

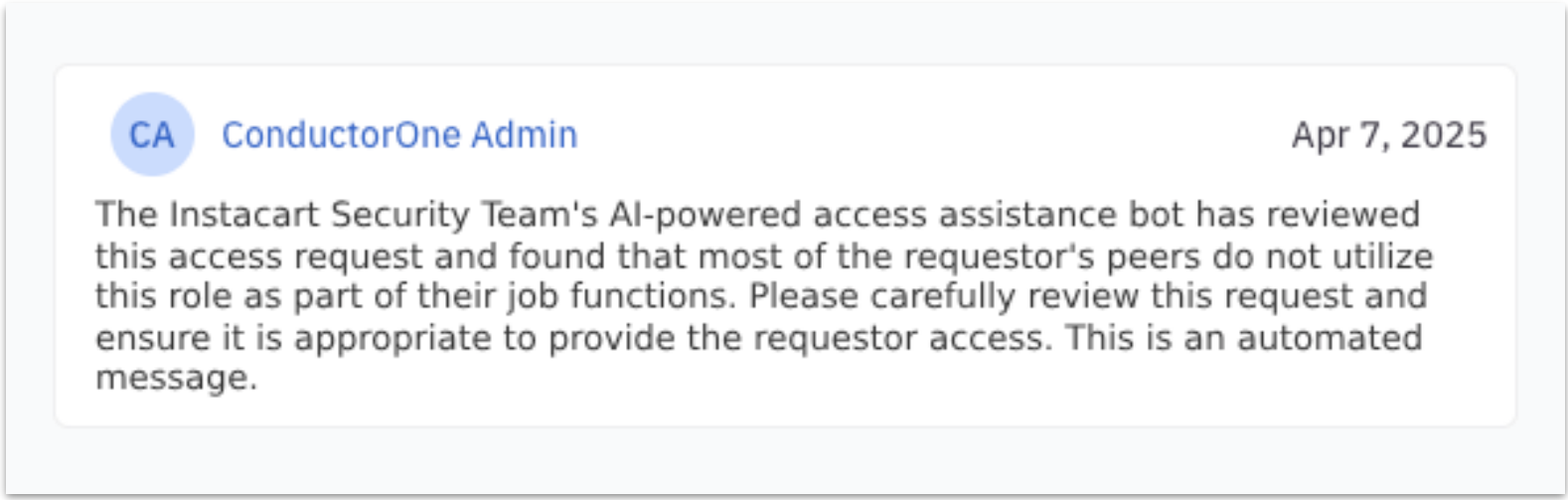


CA ConductorOne Admin Apr 7, 2025

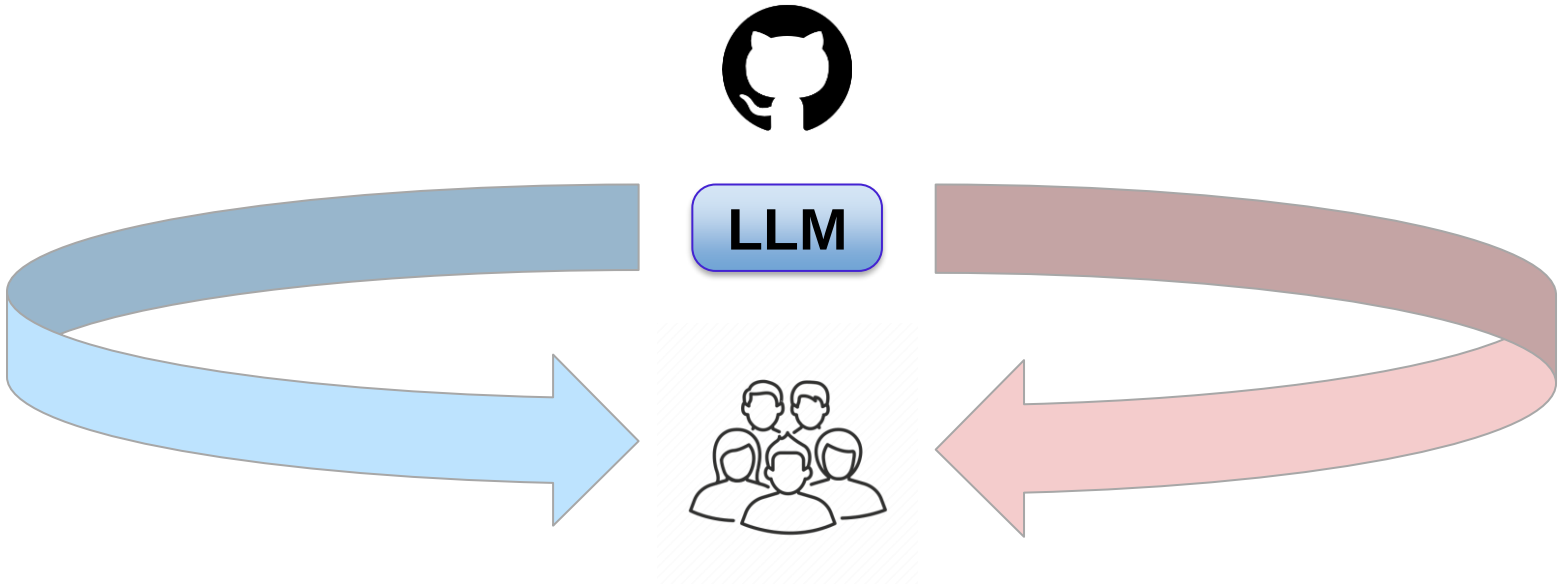
The Instacart Security Team's AI-powered access assistance bot has found that the role AWS-Developer-ReadOnly is less privileged and still provides access to read from 'instacart-example' [S3]. Please request the AWS-Developer-ReadOnly role instead.

Automated Access Review (Gadjit)

- How to trust a bot to automate JIT approvals?
  - Policy-as-code, extended
- Leverage an LLM to do what it does best
  - Feed those results to deterministic Python code thereafter

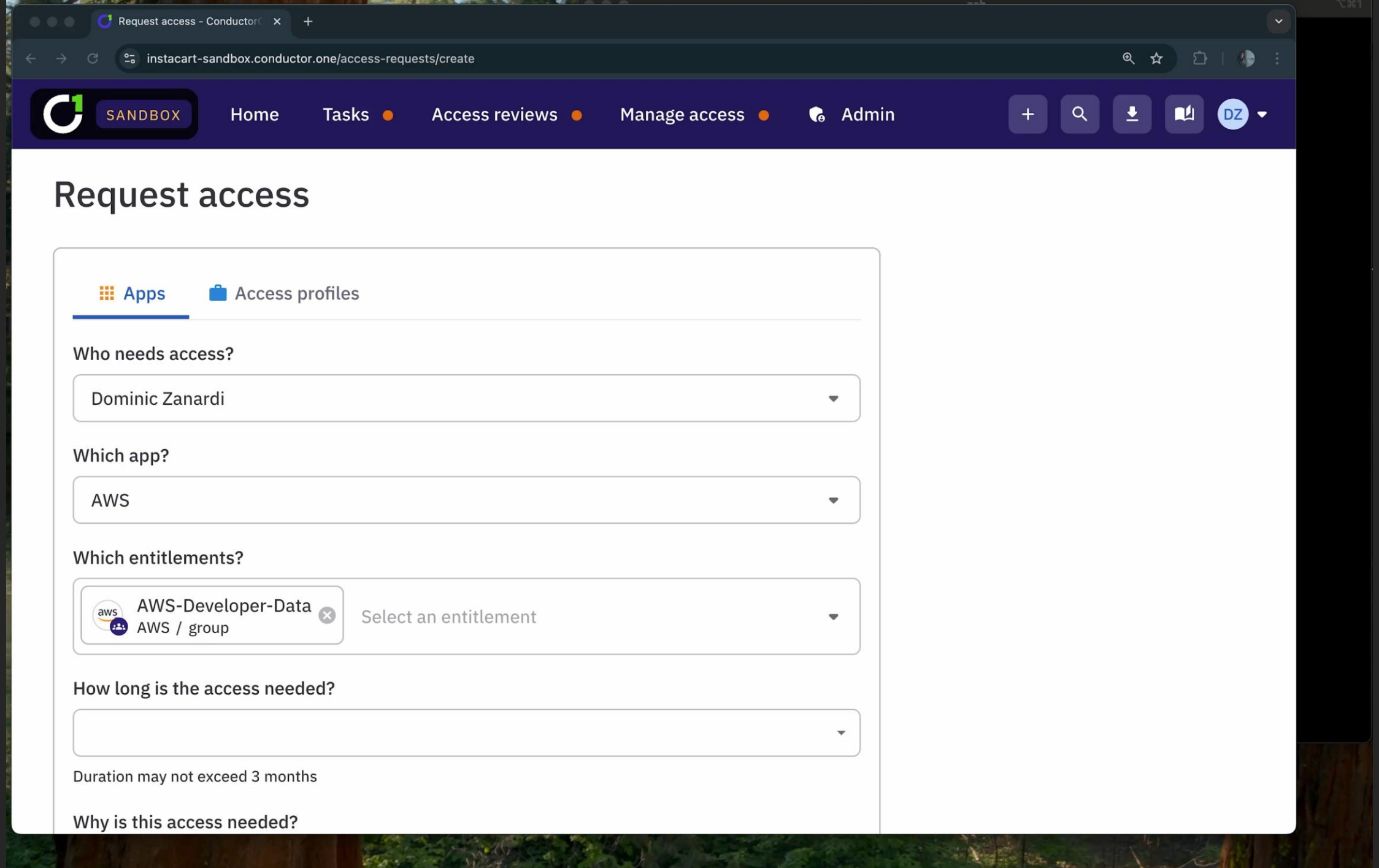

CA
ConductorOne Admin
Apr 7, 2025
The Instacart Security Team's AI-powered access assistance bot has reviewed this access request and found that most of the requestor's peers do not utilize this role as part of their job functions. Please carefully review this request and ensure it is appropriate to provide the requestor access. This is an automated message.

Role Engineering



Add privilege to new resources

Remove privilege left unused


Request access - Conductor
instacart-sandbox.conductor.one/access-requests/create
SANDBOX
Home
Tasks
Access reviews
Manage access
Admin
DZ
Request access
Apps
Access profiles
Who needs access?
Dominic Zanardi
Which app?
AWS
Which entitlements?
AWS-Developer-Data
AWS / group
Select an entitlement
How long is the access needed?
Duration may not exceed 3 months
Why is this access needed?

Attribution: OpenAI & Adobe

Apply 1: Here Be Dragons

- Changing people is hard
- Changing processes is hard
- Auditors
  - Pain of swimming upstream
  - Held to higher standards
  - Humans in the loop

Apply 2: AI Accuracy

- LLMs are great for processing ***massively*** large sets of structured and unstructured data.
- Split up large data sets or accuracy can greatly suffer.
  - Quickly determine what can be eliminated and feed the “top” candidates back in at the final step.
- Take a prompt and ask AI to improve that prompt.

Apply 2: AI Accuracy (continued)

- Today's LLMs can fully understand policy data
- The weak link in the chain is often elsewhere
- Defensive design / defensive coding

Apply 3: AI Privacy

- LLMs know the cloud… but they don’t know you

- Sanitize!

Apply 4: AI Revolution

- AI “Revolution”?
- Reasoning models have completely changed the game.
- Output issues went from model immaturity to operator error in the span of two years.

Attribution: OpenAI & Adobe

RSAC 2025 Conference

Many Voices.
One Community.

Thank You